BILLY J. WILLIAMS, OSB #901366
United States Attorney
District of Oregon
GREGORY R. NYHUS, OSB #913841
Assistant United States Attorney
greg.r.nyhus@usdoj.gov
1000 S.W. Third Avenue, Suite 600
Portland, OR 97204-2902
Telephone: (503) 727-1000
Facsimile: (503) 727-1117
Attorneys for United States of America

UNITED STATES DISTRICT COURT

DISTRICT OF OREGON

UNITED STATES OF AMERICA	**3:13-CR-00064-HZ** **3:14-CR-00190-HZ**
v.	
CYRUS ANDREW SULLIVAN,	**GOVERNMENT'S HEARING MEMORANDUM**
Defendant.	

The United States of America, by Billy J. Williams, United States Attorney for the District of Oregon, through Gregory R. Nyhus, Assistant United States Attorney (AUSA) for the District of Oregon, provides this memorandum of points and authorities for the Court's consideration in the above-entitled matter.

I. BACKGROUND

Defendant is scheduled to appear before this Court on June 7, 2017, for a show cause hearing to determine whether to revoke defendant's term of supervised release. Defendant was convicted of Making Threatening Communications (3:13-CR-00064-HZ) on July 18, 2013, convicted of Assaulting a Federal Employee on November 3, 2014 (3:14-CR-00190-HZ) and placed on a term of supervised release on each matter to run concurrently and the general terms

and conditions of supervision previously adopted by the Court were imposed. At a hearing held on October 11, 2016, defendant's conditions were modified to include a special condition requiring him to participate in the U.S. Probation computer monitoring program.

II. ALLEGATIONS

The government alleges defendant violated the terms and conditions of his supervision as specified:

A. Making Threatening Communications (3:13-CR-00064-HZ)

Special Condition 7: Failing to participate in the U.S, Probation Office's computer monitoring program. On December 3, 2016, defendant installed the software used by U.S. Probation to monitor his computer and Internet activity. Defendant received a new computer for Christmas, installed the monitoring software on December 28, 2016, and later posted derogatory information about the software company on the Internet. On December 30, 2016, he uninstalled the software, but continued to make use of the Internet, as evidenced by e-mails he sent to the computer monitoring company on January 4, 2017, and later, by creating his website copblaster.com. The computer monitoring company believes defendant used an unmonitored computer to search the Internet for content that is not accessible using the monitoring software as the complaints defendant has made to the monitoring company reference blocked websites. The company advises that the blocks are utilized to maintain the integrity of the technologies and the safety of staff.

On January 11, 2017, Internet Probation & Parole Control (IPPC), the monitoring company, confirmed that defendant's computer had been unmonitored since December 30, 2016.

On that same date, defendant advised his computer did not have to be *monitored* by computer monitoring software, but only be *connected* to a monitoring program. USPO Preuitt directed defendant to disable his Internet capability. Instead of complying with USPO Preuitt, as defendant later acknowledged, that he created the website copblaster.com and on February 4, 2017, defendant posted an article about "A.K" on his website

Special Condition 10: Having contact with A.K. (the victim identified in the presentence report), by email, text or any other electronic means, in person, by telephone, through correspondence or a third party unless approved in advance by the probation officer. On February 4, 2017, defendant posted on his website an article about and addressed to A.K. which included a video in which he addressed her directly. While defendant did not directly contact A.K., defendant reasonably anticipated that either USPO Preuitt, who had an obligation to notify the victim and object of defendant's threats, of the communication posted online.

Standard Condition 8: Failure to follow the instructions of a probation officer. Defendant defied USPO Preuitt's directives to stop using the Internet, refused to follow directives to seek and obtain regular employment at a lawful occupation, and failed to complete logs demonstrating such efforts, all as directed by USPO Preuitt.

Standard Condition 10: Failure to work regularly at a lawful occupation. On December 20, 2017, defendant agreed to begin a job search and was provided with job search logs with the directive to submit the logs to USPO Preuitt. As of January 24, 2017, defendant had not completed any job search logs. After this failure, defendant was assigned to a job search specialist with the probation office on January 30 and again on February 6, 2017, but on

February 23, 2017, defendant had not found employment nor had he completed any job search logs.

B. Assaulting a Federal Employee (3:14-CR-00190-HZ)

Standard Condition 8: Failure to follow the instructions of the probation officer. The allegations above are incorporated here.

Standard Condition 10: Failure to work regularly at a lawful occupation. Again, the allegations above are incorporated here.

III. WITNESSES

The government anticipates calling USPO Matt Preuitt as the principle witness. The government anticipates offering as evidence statements made by defendant to USPO Preuitt during the course of his supervision. The government also plans to offer a hard copy of the website copblaster.com copied from the Internet.

The government also anticipates calling Judy Hogaboom to testify about the monitoring software generally, the nature of the blocks used by the software and her discovery of Internet postings attributed to defendant. At this time, the government does not anticipate offering documents through her. Both the government and the defendant have stipulated to receive her testimony by telephone. A phone number will be provided to the Court in advance of the hearing.

IV. RECOMMENDATION

Upon a finding that defendant has violated the terms of his supervision, both the government and USPO Preuitt recommend that defendant's supervised release be revoked and

that he be committed to the custody of the Bureau of Prisons for 11 months on each matter, to be served concurrently, to be followed by a reimposed term of supervision of 24 months.

The government supports U.S. Probation's recommendation that new or modified special conditions be added, which are summarized below (the numbers reference the corresponding recommended condition set forth in the Second Amended Supervision Violation Recommendation):

> 1) You must not access the Internet except as specifically authorized by the Probation Office in advance and may include monitoring at their discretion;
>
> 2) You must not possess and/or use computers (as defined in 18 U.S.C. § 1030(e)(l)) or other electronic communications or data storage devices or media except as approved in writing and in in advance by the Probation Officer;
>
> 3) You are prohibited from posting, and shall remove or cause the removal of any Internet posting, blog entry, comment or other publicly accessible bulletin board which was made by defendant and which refers to "IPPC" or "paycomputermonitoring.com" that identifies any exploit, workaround, vulnerability or method by which to defeat or avoid the intended operation of monitoring software;
>
> 4) You are prohibited from accessing any on-line computer service and/or directing third parties to do so on his behalf at any location (including employment or education) without the prior written approval of the U.S. Probation Officer;
>
> 5) (Original) You shall not own or operate, directly or indirectly, any former website, including "STDCarriers.com," "nolimitlist.com," or any similar website that offers reputation management services or otherwise involves the removal of names, titles, identities, phone numbers, email addresses, or any other personal information from such websites or other publications, whether or not payment of money is required, without the prior written approval of the U.S. Probation Officer;
>
> 6) (Modified) You shall have no contact with A.K. (the victim identified in the presentence report in case number 3:14-CR-00190), by email, text, or any other electronic means, in person, by telephone, through correspondence or a third party

unless approved in advance by the Probation Officer. The defendant shall not post any written article, photograph or video about A.K. on any electronic medium;

7) You shall have no contact with W.S. (the victim identified in the presentence report in case number 3:13-CR-00190) [*sic* 3:14-CR-00190] by email, text, or any other electronic means, in person, by telephone, through correspondence or a third party unless approved in advance by the probation officer. The defendant shall not post any written article, photograph or video about W.S. on any electronic medium;

8) (Modified) You must participate in a mental health treatment program and follow the rules and regulations of that program. The Probation Officer, in consultation with the treatment provider, will supervise your participation in the program (provider, location, modality, duration, intensity, etc.);

9) (Modified) You must take all mental health medications that are prescribed by your treating physician or prescriber;

10) You shall participate in an updated psychiatric evaluation;

11) (Modified) You must not use or possess alcohol;

12) (Modified) You shall remove and/or facilitate the removal of all websites referring to A.K. (the victim identified in the presentence report in case number3:14-CR-00190);

13) You shall remove and/or facilitate the removal of all websites referring to W.S. (the victim identified in the presentence report in case number 3:13-CR-0064); and

14) You shall remove and/or facilitate the removal of the website copblaster.com.

V. LEGAL ISSUES

A. Copblaster.com Removal

Defendant published the personal information of many "covered persons" involved in interactions with defendant and his previous convictions. *See* www.copblaster.com. A "covered person" includes "any officer or employee of the United States or of any agency in any branch of the United States Government," or, "a State or local officer or employee whose restricted

personal information is made publicly available because of the participation in, or assistance provided to, a Federal criminal investigation by that officer or employee." 18 U.S.C. § 1114, 18 U.S.C. § 119(b)(1)(D).

Although defendant's vitriolic posts to his website contain restricted information relating to covered persons, but likely do not rise to violating a federal statute, defendant should be foreclosed from the republication and presentation of personally identifying information in a context which encourages a potentially violent response.

The individual posts do not contain threats, intimidation, or incitements to commit violent crimes against the covered persons and there is not a likely violation of 18 U.S.C. § 119. On the homepage of CopBlaster, however, defendant states the purpose of the site is "the benefit of knowing that their persecutors will finally have to answer to a higher court . . . of public opinion, god's court, allah's court, Bob's court, or whatever you want to call it." Member Benefits, https://copblaster.com/ (last visited April 7, 2017). While this could constitute a threat, most courts seem to take a literal, true threat approach, although innocuous language which may encourage action in some contexts may indeed constitute a threat. *See United States v. McNeil*, 2017 WL 106567 (N.D. Ohio Jan. 11, 2017) (home addresses of military personnel along with a post instructing, "know that it is wajib to kill these kuffar . . . [k]ill them in their own lands, behead them in their own homes, stab them to death as they walk their streets thinking they are safe).

Though the information posted by defendant on his website is publicly available, aggregating and reposting the information in such a context creates an increased risk that *others*

may act. Congress enacted Section 119 as part of the "Court Security Improvement Act" of 2007 (Act). The purpose of the Act was "to protect judges, prosecutors, witnesses, victims, and their families []." H.R. Rep. No. 110-218, pt. 1, at 827 (2007). The Act includes a definition of "restricted information" which includes home addresses. 18 U.S.C. § 119(b)(1). This is because the Act recognizes that "[t]here are restrictions and risks concerning the disclosure of a [covered persons] home address." *Boyd v. Rue*, 2010 WL 3824106, 1 (D. Mass. Sept. 27, 2010) (identifying concern with supplying pro se inmate with USAO prosecutor's home address for service of notice).

The context and content in which the information is relayed, however, is intentionally aimed at harassing and vexing those he has perceived to have harmed him. For example, defendant uses threats to expose others on his website during outbursts in custody when he is not getting his way. The individuals who are the targets of his ire are individuals whose job necessarily exposes them to circumstances which concerns their individual safety. While the information defendant posted about sheriff's deputies, Bureau of Prisons employees, and U.S. Attorney's Office prosecutors is otherwise publicly known, the information is still "restricted" according to the statute because of the designation of those individuals as "covered persons."

Like defendant's former websites that contributed to his convictions, should defendant be allowed to continue to operate his website, it would put defendant in a place where he is likely to reoffend and commit additional crimes. Defendant does not cope with conflict well, and the website invites conflict. Defendant should therefore be compelled to remove it.

///

B. Internet Restriction

Proposed conditions of supervision 1, 2 and 4 combine to significantly curtail defendant's Internet access. The language does not prevent *all* Internet access but significantly restricts access to circumstances that are amenable to close supervision and regulation. Even though defendant initially agreed to Internet monitoring, defendant not only abused the privilege of access but also exploited and published a defect in the software, thereby encouraging wide-scale disregard for monitoring conditions.

The government recognizes that because of the vital nature of Internet use in today's world, supervised release conditions banning all Internet access without prior approval from a probation officer are generally too severe a restraint on a defendant's liberty. *U.S. v. LaCoste*, 821 F.3d 1187, 1191 (9th Cir. 2016). Such bans make it "difficult to participate fully in society and the economy." *Id.* However, permitting such conditions are appropriate in only two scenarios: first, when the internet was "essential or integral to the offense of conviction," or second, when the internet played no role in the offense of conviction, but the defendant has "a history of using the internet to commit other offenses." *Id.* If imposition of the Internet ban involves "no greater deprivation of liberty than is reasonably necessary," protects the public, and adequately deters defendant's criminal conduct, the ban is appropriate. *See* 18 U.S.C. § 3583(d)(2); 18 U.S.C. § 3553(a)(2)(B) & (C).

Defendant is on supervised release for crimes related to the Internet. On April 15, 2013, defendant pled guilty to knowingly transmitting in interstate or foreign commerce communication to containing a threat to injure the person of another, in violation of

18 U.S.C.§ 875(c). Defendant threatened to kill a woman who had previously contacted him via the Internet in response to having her personal information posted on defendant's website, stdcarriers.com. The threat was the culmination of a chain of emails between defendant and his victim. The Internet was an essential and integral part of the defendant's offense.

While under his current release conditions, defendant has posted additional information about his victim online, created a website with the names and personal information of officials involved with his case, and disabled the Internet monitoring software on his computer. A total Internet ban, a revision to the less restrictive condition, is in response to defendant's repeated violations of a less restrictive condition.

While the essential nature of the Internet to defendant's conviction is enough to satisfy the Ninth Circuit, a look at defendant's subsequent Internet activity, after the imposition of the initial condition of supervision, should further inform the Court. Revising the supervision condition to ban all Internet access without prior approval from a probation officer is reasonable.

Defendant's sophisticated computer skills and encouragement of others to circumvent monitoring software are "particular and identifiable characteristics" that support a revision of his supervised release condition to a total ban on Internet use. Other circuits have addressed the issue in cases remarkably similar to defendant.

In *U.S. v. Johnson*, the Second Circuit upheld a ban where the defendant had sophisticated computer skills that would enable him to circumvent monitoring software. *U.S. v. Johnson*, 446 F.3d 272, 282–283 (2nd Cir. 2006). Here, defendant has done just that, even going so far as to brag about disabling the monitoring software to his probation officer.

Defendant has also posted a "how to" on copblaster.com; a website he created after release, informing others under supervision by probation how to circumvent the monitoring software. How to Disable Internet Probation and Parole Control Software (https://copblaster.com/blast/48/how-to-disable-internet-probation-and-parole-control-software (last visited March 31, 2017)). The implications of this posting are far-reaching and troublesome. The Fifth Circuit has affirmed a ban where a defendant used the Internet to advise and encourage others to commit crimes similar to his underlying offense. See *U.S. v. Paul*, 274 F.3d 155, 169 (5th Cir. 2001) (affirming a total ban where a child pornography offender had used the internet to seek out fellow pedophiles and advise them on how to obtain access to children). While the present facts may not be as lascivious as those in *Paul*, defendant's disabling of the monitoring software and step-by-step guide for others to do the same should not be without consequence. The offenders who benefit from defendant's advice on how to violate supervision conditions related to Internet access may very well be committing such crimes.

Defendant's repeated, and successively more bold, violations of his supervised release are clear indications that severe restrictions may be the only way to prevent future violations.

Dated this 6th day of June 2017.

Respectfully submitted,

BILLY J. WILLIAMS
United States Attorney

s/ Gregory R. Nyhus
GREGORY R. NYHUS, OSB #913841
Assistant United States Attorney